PRIVACY IMPACT ASSESSMENT (PIA)

For the

Authentication Gateway Services (AGS)

Enterprise Directory Services (EDS)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

□ (1) Yes, from members of the general public.

□ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

□ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

□	**New DoD Information System**	□	**New Electronic Collection**
□	**Existing DoD Information System**	☒	**Existing Electronic Collection**
□	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	**Yes, DITPR**	Enter DITPR System Identification Number	3172
☒	**Yes, SIPRNET**	Enter SIPRNET Identification Number	3172
□	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

□ **Yes** ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** □ **No**

If "Yes," enter Privacy Act SORN Identifier K890.15 DoD

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

5 U.S.C. 301, Departmental Regulation; DoD Directive 5105.19, Defense Information Systems Agency (DISA); DoD Chief Information Officer Memorandum for Director, Defense Information Systems Agency (DISA), Enterprise Directory Services Roadmap for the Department of Defense, 2 May 2005.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

AGS is an authentication solution that acts as a reverse proxy to allow applications to meet the DoD requirement that systems and applications support Public Key Infrastructure (PKI) authentication. Data collected includes: persona username.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Access to the type and amount of data is governed by privilege management software and policies developed and enforced by Federal government personnel. Defense-in-Depth methodology is used to protect the repository and interfaces, including (but not limited to) multi-layered firewalls, Secure Sockets Layer/Transport Layer Security connections, directory access control lists, file system permissions, intrusion detection and prevention systems and log monitoring. Complete access to all records is restricted to and controlled by certified system management personnel, who are responsible for maintaining the system integrity and the data confidentiality.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. ITSM and milCloud

☒ **Other DoD Components.**

Specify. ARMY

□ **Other Federal Agencies.**

Specify.

□ **State and Local Agencies.**

Specify.

□ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

□ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Individuals may object to the collection of PII by not providing the requested information, however, this information is required to gain access to the network.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Individuals are provided a consent form and they may choose not to sign it, however, this consent is required to gain access to the network.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement**	☐ **Privacy Advisory**
☐ **Other**	☐ **None**

Describe each applicable format.	PRIVACY ACT STATEMENT Authority for maintenance of system: 5 U.S.C. 301, Departmental Regulation; DoD Directive 5105.19, Defense Information Systems Agency (DISA). Purpose(s): Form is used to establish a Local Area Network (LAN) Account. This includes the level of security clearance and level of access to classified information that has been authorized. Information is used by commanders, supervisors, and security managers to ensure that individuals who are granted access to classified information have been properly investigated, cleared, and have a definite need-to-know. The DoD Blanket Routine Uses published at the beginning of the DISA's compilation of systems of records notices apply to this system. In addition to those disclosures generally permitted under 5 USC 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside of DoD as a routine use pursuant 5 USC 552a(b)(3) as follows: The 'Blanket Routine uses' set forth at tthe beginning of the DISA's compilation of systems of records notices apply to this system.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☒ Name
□ Other Names Used
□ Social Security Number (SSN)
□ Truncated SSN
□ Driver's License
□ Other ID Number
□ Citizenship
□ Legal Status
□ Gender
□ Race/Ethnicity
□ Birth Date
□ Place of Birth
□ Personal Cell Telephone Number
□ Home Telephone Number
□ Personal Email Address
□ Mailing/Home Address
□ Religious Preference
□ Security Clearance
□ Mother's Maiden Name
□ Mother's Middle Name
□ Spouse Information
□ Marital Status
□ Biometrics
□ Child Information
□ Financial Information
□ Medical Information
□ Disability Information
□ Law Enforcement Information
□ Employment Information
□ Military Records
□ Emergency Contact
□ Education Information
□ Other

If "Other," specify or explain any PII grouping selected.

Categories of records in the system: persona username (PUN), Common Name, Mail Nickname, SUR name

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

All information is collected and correlated from existing DoD information Systems, specifically from Dod Component Active Directory databases, eth DoD PKI Global Directory Service (GDS), and the Defense manpower Data Center (DMDC) Defense Enrollment and Eligibility Repository System (DEERS).

(3) How will the information be collected? Indicate all that apply.

□ **Paper Form**

□ **Telephone Interview**

□ **Email**

□ **Information Sharing - System to System**

□ **Face-to-Face Contact**

□ **Fax**

□ **Web Site**

☒ **Other**

Automated system-to-system directory data synchronization methodologies.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

Purpose(s): To provide a DoD authentication/authorization capability offering a single source from which to obtain identity and contact information about Combatant Command, Service, and Agency personnel as well as an enterprise level attribute service. EDS will support the warfighter's mission by providing access, via controlled interfaces, to DoD personnel contact information and when requested by approved DoD applications, to identity attributes, and to support authorization decisions.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Purpose(s): To provide enterprise level attribute service for authorization decisioning and support the warfighter's mission by providing access, via controlled interfaces, to DoD personnel contact information and when requested by approved DoD applications, to identity attributes, and to support authorization decisions.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

□ **Yes** ☒ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

☒ Users ☒ Developers ☒ System Administrators ☒ Contractors

☐ Other

If "Other," specify here.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

☒ Security Guards	☒ Cipher Locks
☒ Identification Badges	☐ Combination Locks
☒ Key Cards	☒ Closed Circuit TV (CCTV)
☐ Safes	☒ Other

Safeguards: Access to the type and amount of data is governed by privilege management software and policies developed and enforced by Federal government personnel. Defense-in-Depth methodology is used to protect the repository and interfaces, including (but not limited to) multi-layered firewalls, Secure Sockets Layer/Transport Layer Security connections, Directory access control lists, file system permissions, intrusion detection and prevention systems and log monitoring. Complete access to all records is restricted to and controlled by certified system management personnel, who are responsible for maintaining the EDS system integrity and the data confidentiality.

(2) Technical Controls. Indicate all that apply.

☒ User Identification	☐ Biometrics
☒ Password	☒ Firewall
☒ Intrusion Detection System (IDS)	☒ Virtual Private Network (VPN)
☒ Encryption	☒ DoD Public Key Infrastructure Certificates
☐ External Certificate Authority (CA) Certificate	☒ Common Access Card (CAC)
☐ Other	

If "Other," specify here.

(3) Administrative Controls. Indicate all that apply.

☒ **Periodic Security Audits**

☒ **Regular Monitoring of Users' Security Practices**

☒ **Methods to Ensure Only Authorized Personnel Access to PII**

☐ **Encryption of Backups Containing Sensitive Data**

☒ **Backups Secured Off-site**

☐ **Other**

If "Other," specify here.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

☐ **Yes. Indicate the certification and accreditation status:**

☒	**Authorization to Operate (ATO)**	**Date Granted:**	2 Dec 2013
☐	**Interim Authorization to Operate (IATO)**	**Date Granted:**	
☐	**Denial of Authorization to Operate (DATO)**	**Date Granted:**	
☐	**Interim Authorization to Test (IATT)**	**Date Granted:**	

☐ **No, this DoD information system does not require certification and accreditation.**

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Collection: Individuals provide information for application resource authorization
Use: Disseminate account and work contact information
Processing: Electronic data collection is provided for individuals to complete account creation requirements
Retention: Disposition pending (until National Achieves and Records Administration approves retention and disposal schedule, records will be treated as permanent).
Disclosure: Individual is provided a Privacy Act Statement and acknowledges use of individuals' information
Destruction: Disposition pending (until National Achieves and Records Administration approves retention and disposal schedule, records will be treated as permanent).

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

Information is used for official use only. Role based access restricts use by unauthorized users of the system. Measures include CAC enabled, firewalls, SSL (https), intrusion detection, and port security. Unauthorized attempts to upload information or change information on servers are strictly prohibited and may be punishable by law, including the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act. Monitoring includes active attacks by authorized DOD entities to test or verify the security of this system.

Records are maintained in a secure, limited access, and monitored work area. Physical entry by unauthorized persons is restricted by the use of locks, guards, and administrative procedures. Access to personal information is restricted to those who require the records in the performance of their official duties. Access to computer records is further restricted by the use of passwords. All personnel whose official duties require access to the information are trained in the proper safeguarding and use of the information and received Information Assurance and Privacy Act training. Paper records are marked "FOUO-PRIVACY ACT PROTECTED DATA" and stored in a locked container when not in use.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

Describe here.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature	ABRAMS.RICHARD.ALLEN.1059484512 Digitally signed by ABRAMS.RICHARD.ALLEN.1059484512 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DISA, cn=ABRAMS.RICHARD.ALLEN.1059484512 Date: 2013.08.02 11:52:04 -04'00'
Name:	Richard A. Abrams
Title:	Branch Chief
Organization:	EIS
Work Telephone Number:	301-225-8717
DSN:	
Email Address:	richard.a.abrams.civ@mail.mil
Date of Review:	
Other Official Signature (to be used at Component discretion)	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	

Other Official Signature (to be used at Component discretion)	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	
Component Senior Information Assurance Officer Signature or Designee	Alma J. Miller
Name:	Alma J. Miller
Title:	Chief, Information Assurance Division
Organization:	[redacted] MAE
Work Telephone Number:	301-225-8244
DSN:	
Email Address:	alma.j.miller2.civ@mail.mil
Date of Review:	
Component Privacy Officer Signature	Jeanette M. Weathers-Jenkins
Name:	Jeanette M. Weathers-Jenkins
Title:	DISA Privacy Officer
Organization:	CIO
Work Telephone Number:	301-225-8158
DSN:	
Email Address:	jeanette.m.weathersjenkin.civ@mail.mil
Date of Review:	

Component CIO Signature (Reviewing Official)	Sherry Z Baker VICE CIO
Name:	For David B. Bennett
Title:	Chief Information Officer
Organization:	CIO
Work Telephone Number:	301-225-8000
DSN:	
Email Address:	david.b.bennett10.civ@mail.mil
Date of Review:	

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.